Fresenius Medical Care

February 8, 2007

Ms. Lauren Noether
Bureau Chief Consumer Protection
33 Capitol Street
Concord, NH 03301

Dear Ms. Noether:

Fresenius Medical Care Holdings, Inc., doing business as Fresenius Medical Care North America (FMCNA) is providing notice in accordance with New Hampshire Rev. Stat. § 359-C:20, that on December 13, 2006 a laptop computer was stolen from the locked car of an FMCNA employee. The car was parked at a local restaurant and the window was smashed to gain access. The theft occurred in Waltham, Massachusetts and a police report was filed.

On February 9, 2007 FMCNA plans to send the attached notice to the one New Hampshire resident affected. The notice more fully describes the nature of the breach.

Please let me know if you have any questions or if I can be of additional assistance.

Sincerely,

Rick King

Rick King
Privacy and Security Officer
Fresenius Medical Care North America

Fresenius Medical Care

February 9, 2007

First Name, Last Name
Address 1
Address 2
City, State Zip

Private and Confidential Communication

Dear Salutation Last Name,

I am writing to inform you of a recent event that may impact you and your personal information as a current or past patient of Fresenius Medical Care North America (FMCNA).

On December 13, 2006 a laptop computer was stolen from the locked vehicle of an FMCNA employee. The laptop contained the personal information of a number of our patients and the holders of health insurance used to pay for their care. Your information was among the information that was on the stolen computer.

The information disclosed included the following:

- Patient Name
- Date of Birth
- Name of the Insured Person, if Different from the Patient
- Insurance Account Number as of 2004 or earlier
- Insurance Company as of 2004 or earlier
- FMCNA Account Number
- FMCNA Service Location
- Dates of Service
- Services Provided
- Status of Insurance Payments

FMCNA has determined that the Insurance Account Number was frequently the same as, or contained, the patient's Social Security Number. Where the insured person was not the patient, the Insurance Account Number may be the Social Security Number of the insured person, instead of the patient's Social Security Number. For instance, a patient may be covered under his or her spouse's insurance. The Insurance Account Number may be the spouse's Social Security Number. In some instances, there may be no connection between the Insurance Account Number and a Social Security Number. A separate letter is being sent to the holder of the health insurance if that person was not you.

FMCNA takes its responsibility to protect your personal information very seriously, and we apologize for any inconvenience caused to you as a result of these events.

The police were contacted immediately upon discovering the theft, and a police report was made. At this point, the laptop has not been recovered. The computer was password protected using a strong password.

We have no information to date indicating that the information on the computer has been accessed or has been inappropriately used. FMCNA has taken action to prevent someone from being able to access additional FMCNA information using the stolen computer.

Attached please find some actions that you can take to help protect yourself against both financial and medical identity theft.

In addition, FMCNA has arranged to provide you with credit monitoring using the Debix Identity Protection Service for one year free of charge. If you would like to use this service, you may sign up on-line at www.debix.com/FMCNA, or you can complete and return the attached form to Debix Inc. 900 Congress Avenue, Suite 402, Austin, TX 78701 using the enclosed pre-addressed, postage paid envelope. Please refer to the attached flyer for additional information.

If you have questions about this letter, please contact Karen Lopes, Fresenius Medical Services Divisional Privacy and Security Officer, at 1-800-662-1237, extension 4092.

Sincerely,

Bill Numbers
Vice President, Operations Support
Fresenius Medical Care North America

Fresenius Medical Care

Steps You Can Take to Protect Against Financial Identity Theft

The United States Federal Trade Commission ("FTC") recommends that consumers take the following steps when their Social Security number has been stolen, in order to prevent someone from using that information to open new credit accounts in the consumer's name.

1. Call the toll-free fraud number of any of the three nationwide consumer reporting companies listed below and place an **initial fraud alert** on your credit reports.
2. Once you have placed an initial fraud alert on your credit reports, you will then be entitled to one **free credit report** from each of the three nationwide consumer reporting companies.
   - If you plan to use the Debix Identity Protection Service paid for by FMCNA, we recommend that you request a free credit report from one of the nationwide consumer reporting companies now, and request a free credit report from one of the other nationwide consumer reporting companies 60 or more days after you activate the Debix Identity Protection Service. That way, you can confirm that no new unauthorized credit was set up in your name before the Debix Identity Protection Service started, but reported after your first credit report request.
3. **Review your credit reports** to determine if anyone has used your information to open new credit accounts in your name. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address(es), name or initials, and employers are correct.
4. **Stay alert.** The FTC recommends that you review your credit report once every three months for the first year, and annually thereafter. There are commercially available services offered through each of the nationwide consumer reporting companies and major credit cards that can automatically monitor your credit reports and notify you of any changes. FMCNA has arranged to provide you with such a service, the Debix Identity Protection Service, for one year free of charge. If you would like to use this service, you may sign up on-line at www.debix.com/FMCNA, or you can complete and return the attached form to Debix Inc. 900 Congress Avenue, Suite 402, Austin, TX 78701 using the enclosed pre-addressed, postage paid envelope. Please refer to the attached flyer for additional information.

The toll-free fraud number and other contact information for the three nationwide consumer reporting companies are:

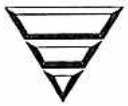
- **Equifax**: 1-800-525-6285; www.equifax.com;
  P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian**: 1-888-397-3742; www.experian.com
  P.O. Box 9532, Allen, TX 75013
- **Transunion**: 1-800-680-7289; www.transunion.com
  Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834

In addition, federal law requires that each of the nationwide consumer reporting companies provide you with a free copy of your credit report, at your request, once every 12 months. These requests can only be made by calling 1-877-322-8228 or by visiting www.annualcreditreport.com.

To obtain more detailed information about how to get free credit reports go to the FTC web site at www.consumer.gov/credit. There you can access the FTC publication "Your Access to Free Credit Reports."

For detailed information on preventing or recovering from identity theft, go to the FTC web site at www.consumer.gov/idtheft. There you can access the FTC publication "Take Charge: Fighting Back Against Identity Theft."

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.consumer.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.



Fresenius Medical Care

Steps You Can Take to Protect Against Medical Identity Theft

Medical Identity Theft may result in fraudulent medical bills that are paid by your insurer or by you. Medical Identity Theft may also result in the inclusion of the identity thief's medical information in your medical records.

Medical Identity Theft may be, but is not always, able to be detected by monitoring your credit report. In order to protect yourself against the potential for medical identity theft, FMCNA recommends that you:

1. Carefully review all Explanation of Benefits (EOB) forms sent to you by your insurer. Look at the services provided and payments made, and confirm that they are for services that you received.
2. Once a year, ask your health care insurer for a list of all benefits that it paid on your behalf. Look at the services provided and payments made, and confirm that they are for services that you received. This can help identify services provided to an identity thief if the thief changed the address to which your statements are mailed.
3. Review your credit file for debts owed to health care providers that were not incurred by you.

If you identify medical services that you believe were not provided to you, contact the insurer or the health care provider immediately.

DEBIX
The Identity Protection Network

DEBIX IDENTITY PROTECTION

Control

Only you know when it's really you applying for credit and when it's not. So Debix gives you the power to approve or reject any and all applications for credit in your name.

Convenience

All you need is a phone. Debix requires every creditor to contact you through our secure, automated phone network before opening any new account.

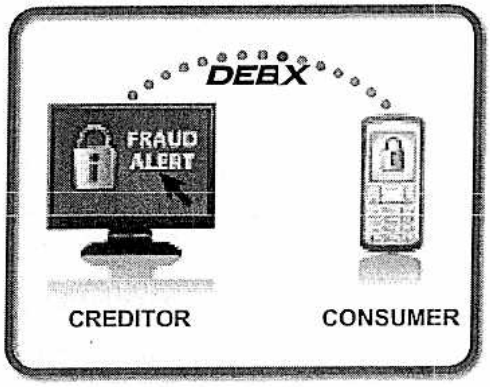
Peace of Mind

Your social security number and other personal information become useless to identity thieves. No one can impersonate you with creditors.

What does it do?

Debix Identity Protection actually stops identity fraud before you become a victim.

You will be contacted on your phone for approval anytime anyone applies for credit in your name.



With Debix Identity Protection it is impossible for thieves to impersonate you even if they have your social security number or other personal information.

Debix Identity Protection shields you by never disclosing your phone number to creditors.

You may elect to have Debix add your phone number to the National Do Not Call Registry so telemarketers do not have permission to call you.

Debix can stop you from receiving pre-approved offers from creditors and insurance companies – a leading cause of fraud.

For one year of Debix Identity Protection paid for by FMCNA, you may sign up on-line at www.debix.com/FMCNA or complete the attached form and mail it in.

DEBIX
The Identity Protection Network

Registration Form

Debix Identity Protection

Personal Information

Legal Name: _____
Last *First* *M.I.* *Suffix (Jr., II)*

Address: _____
Street Address *Apartment/Unit #*

_____
City *State* *ZIP Code*

Cell Phone: ( ) _____ Alternate Phone: ( ) _____

E-mail Address: _____

Social Security Number: _____

Birth Date: _____ Gender : _____

E-Mail Address: _____

Previous Address if Less than 24 months

Address: _____
Street Address *Apartment/Unit #*

_____
City *State* *ZIP Code*

Optional Protections

The following identity protections are highly recommended. Please check the box if you wish to receive these protections.

- ☐ Opt-out of receiving pre-approved and prescreened offers from creditors and insurance companies; a leading cause of fraud.
- ☐ Add your registered phone number to the National Do Not Call Registry so telemarketers do not have permission to call you.

Registration Call

I understand the Debix system will be calling me so that I may record my name, and set my voice key and pin. I would prefer the Debix system call me between:

- ☐ 8am – 5pm CST
- ☐ 5pm – 9pm CST

Signature

Signature: _____

Debix Encrypts all sensitive personal information. Debix will never sell, rent, or intentionally provide your personally identifiable information to any third parties for their marketing purposes.

Please mail this form to Debix, 900 Congress Ave, Suite 402, Austin, TX 78701.